FIG. 1

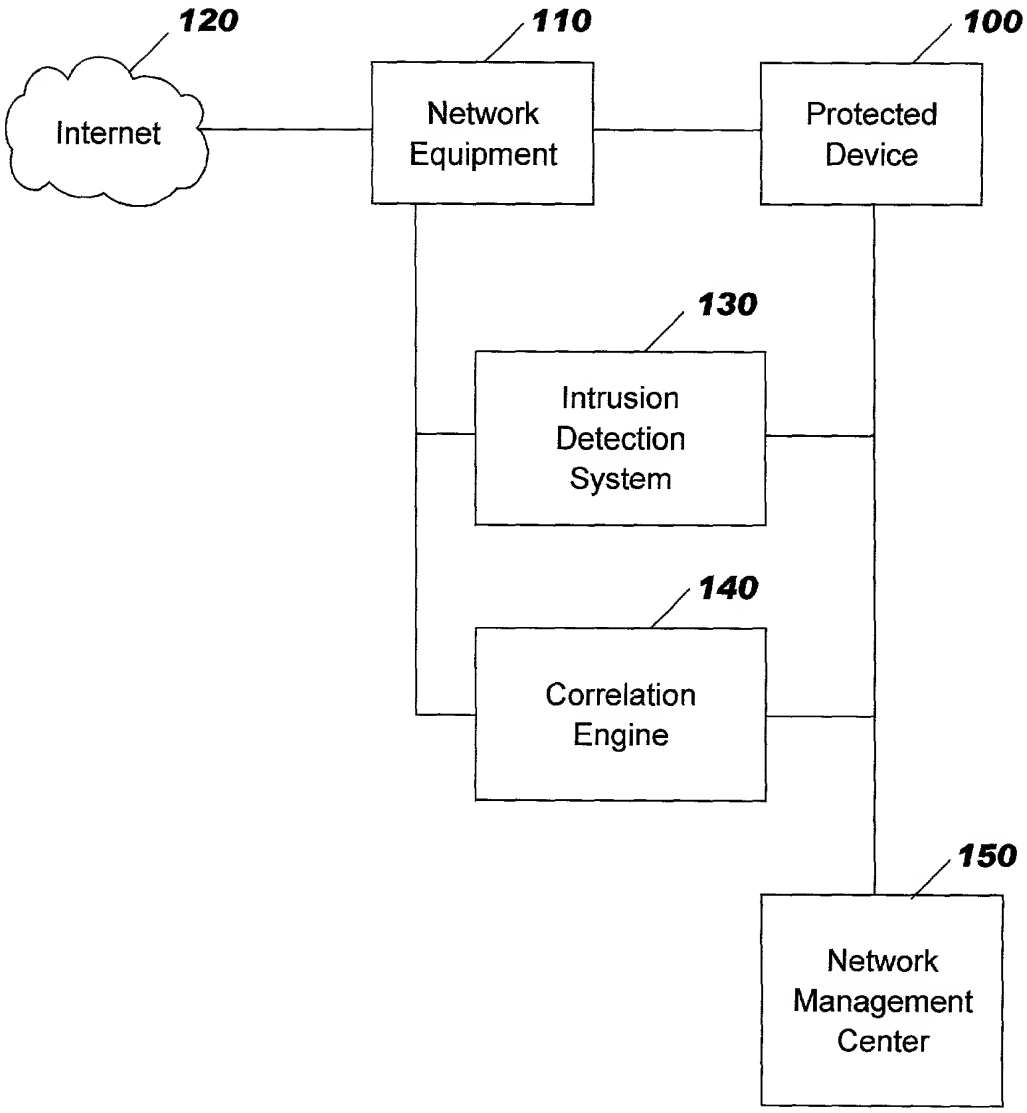

120
110
100
Internet
Network Equipment
Protected Device
130
Intrusion Detection System
140
Correlation Engine
150
Network Management Center

FIG. 2

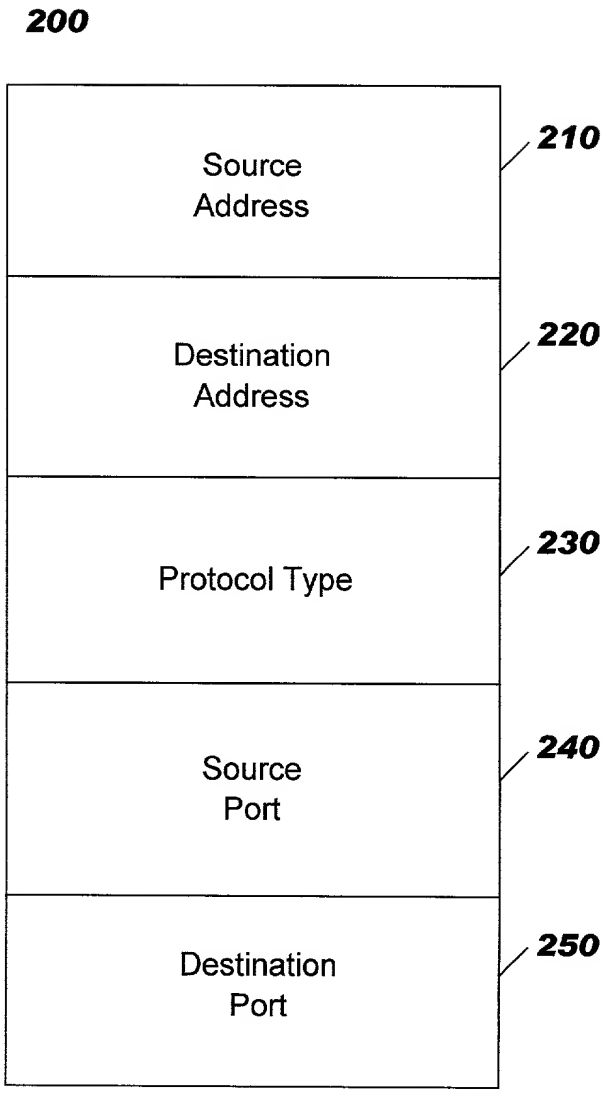

200
Source Address
210
Destination Address
220
Protocol Type
230
Source Port
240
Destination Port
250

FIG. 3

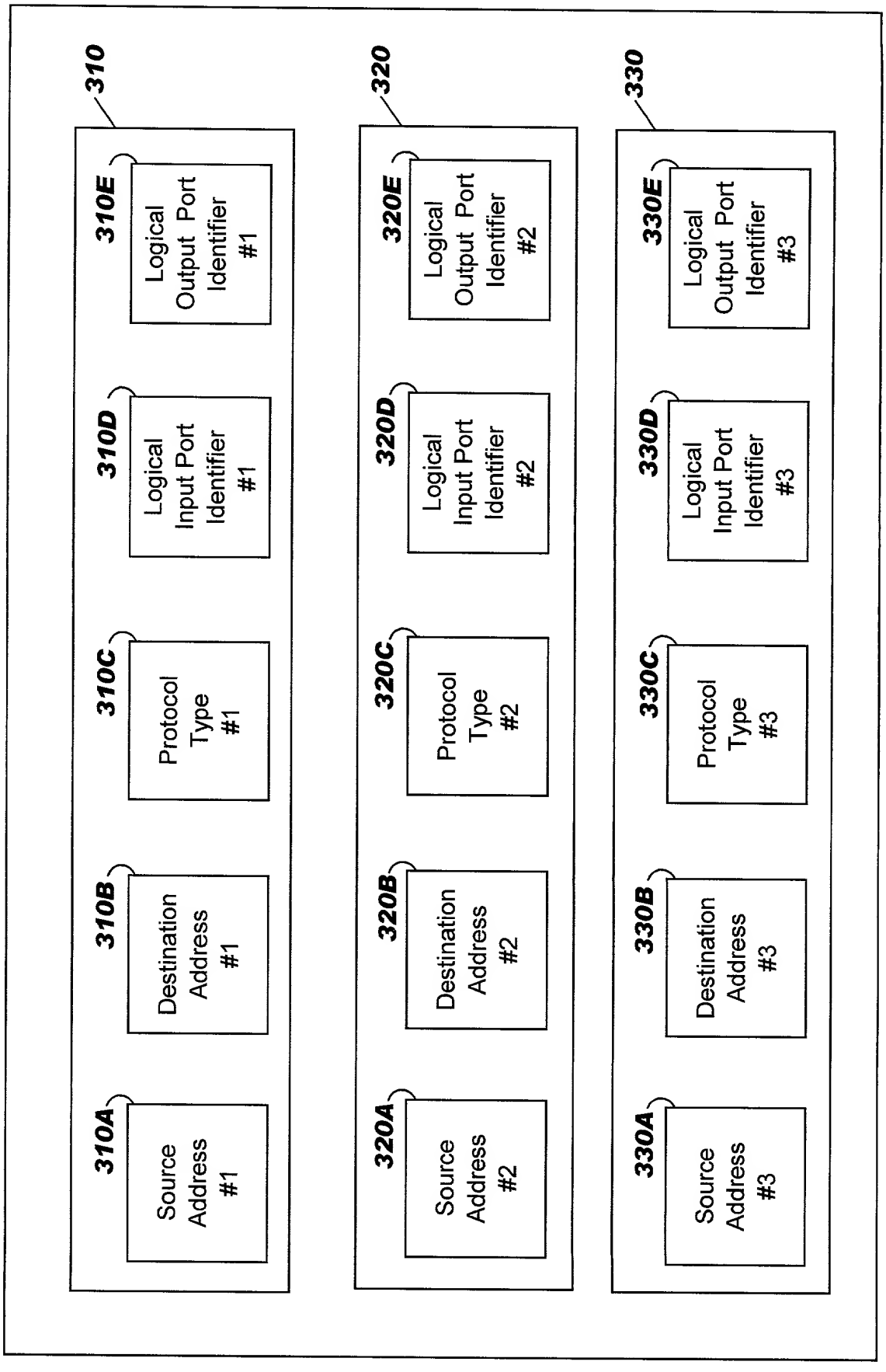

300
310
310A
Source Address #1
310B
Destination Address #1
310C
Protocol Type #1
310D
Logical Input Port Identifier #1
310E
Logical Output Port Identifier #1
320
320A
Source Address #2
320B
Destination Address #2
320C
Protocol Type #2
320D
Logical Input Port Identifier #2
320E
Logical Output Port Identifier #2
330
330A
Source Address #3
330B
Destination Address #3
330C
Protocol Type #3
330D
Logical Input Port Identifier #3
330E
Logical Output Port Identifier #3

FIG. 4

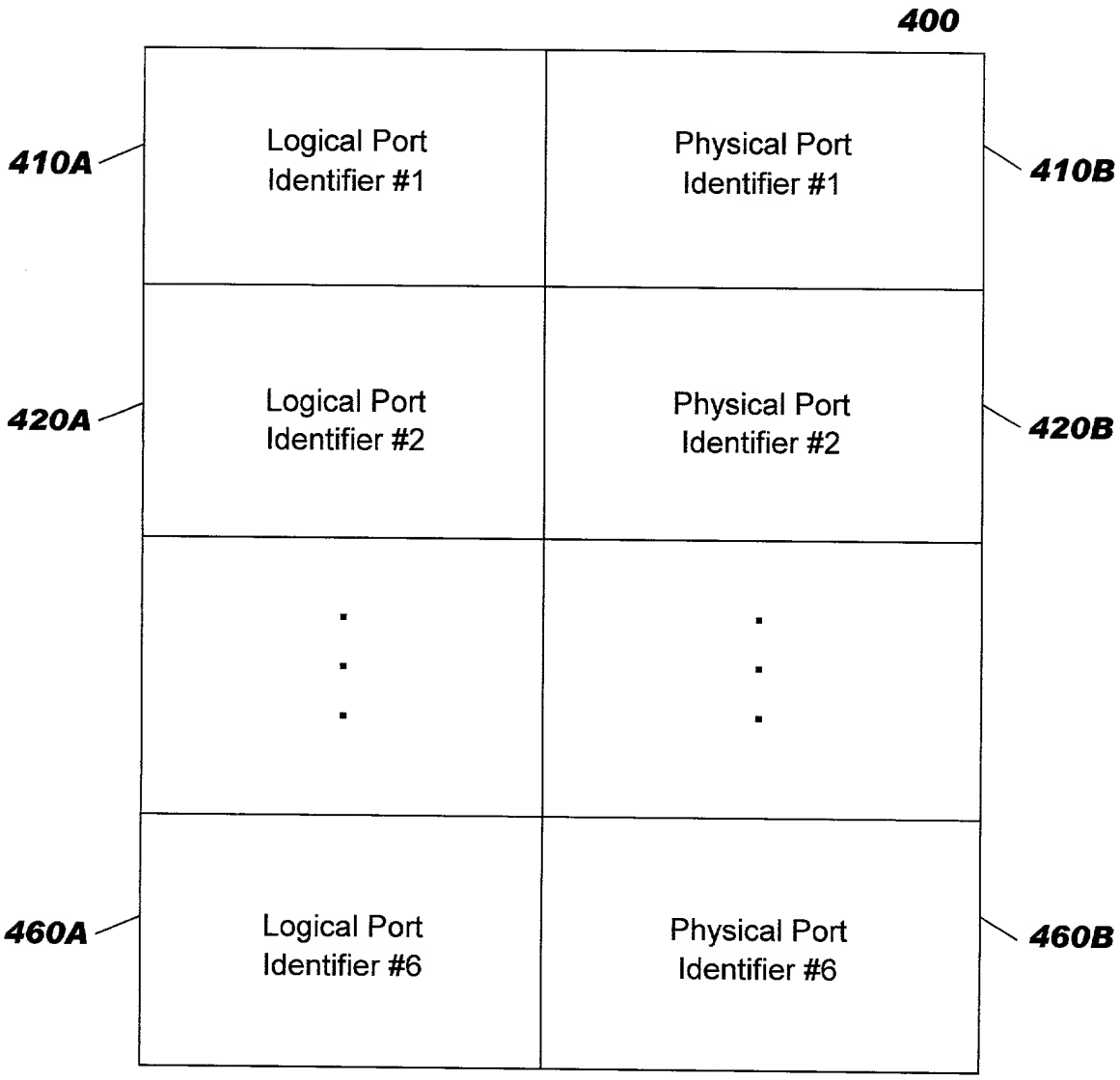
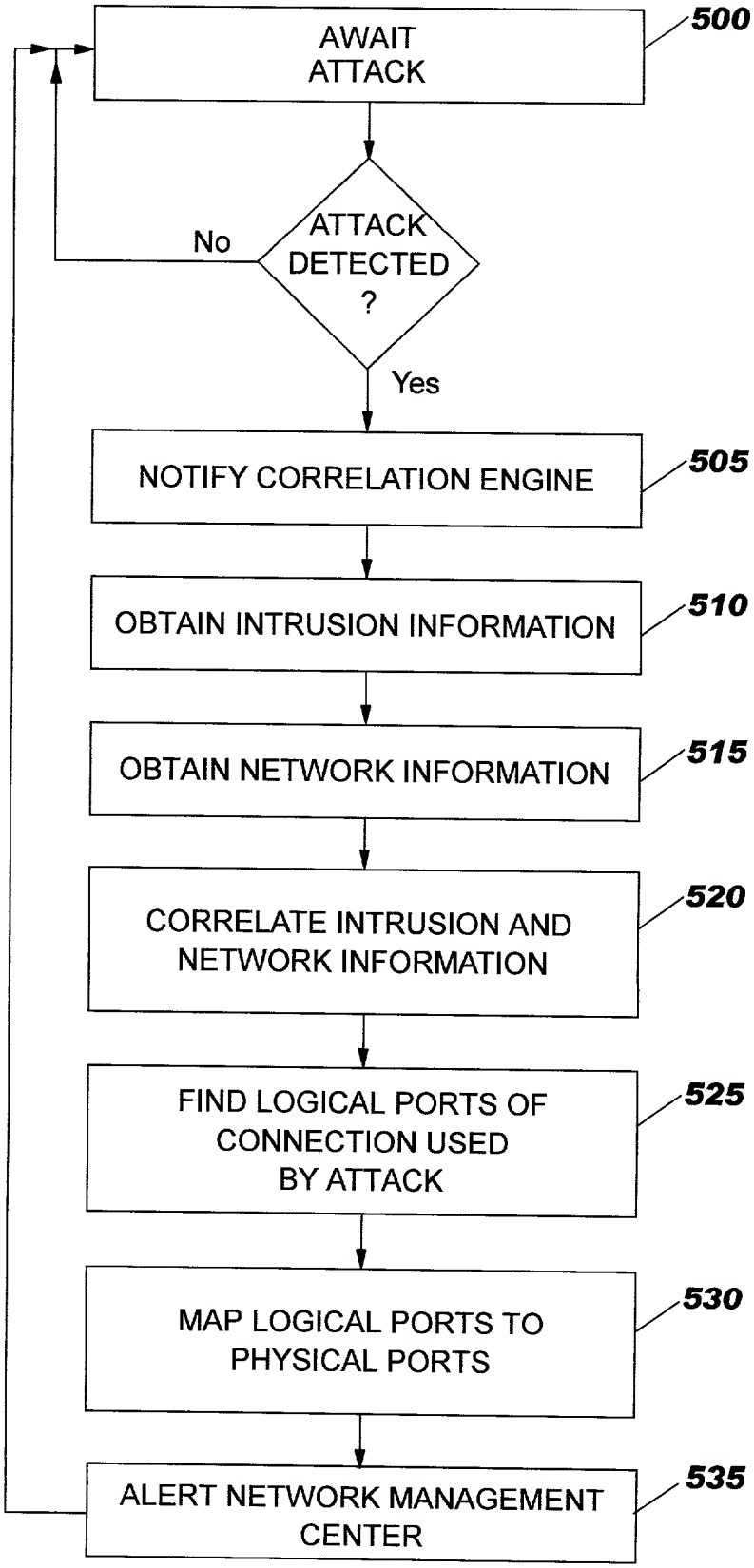

400
410A
Logical Port Identifier #1
Physical Port Identifier #1
410B
420A
Logical Port Identifier #2
Physical Port Identifier #2
420B
460A
Logical Port Identifier #6
Physical Port Identifier #6
460B

FIG. 5


AWAIT ATTACK
500
ATTACK DETECTED ?
No
Yes
NOTIFY CORRELATION ENGINE
505
OBTAIN INTRUSION INFORMATION
510
OBTAIN NETWORK INFORMATION
515
CORRELATE INTRUSION AND NETWORK INFORMATION
520
FIND LOGICAL PORTS OF CONNECTION USED BY ATTACK
525
MAP LOGICAL PORTS TO PHYSICAL PORTS
530
ALERT NETWORK MANAGEMENT CENTER
535